AZ-104Q&As

Microsoft Azure Administrator

Pass Microsoft AZ-104 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/az-104.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company has an Azure Active Directory (Azure AD) tenant named weyland.com that is configured for hybrid coexistence with the on-premises Active Directory domain.

You have a server named DirSync1 that is configured as a DirSync server.

You create a new user account in the on-premise Active Directory. You now need to replicate the user information to Azure AD immediately.

Solution: You restart the NetLogon service on a domain controller.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: B

QUESTION 2

You have an Azure virtual machine named VM1.

You use Azure Backup to create a backup of VM1 named Backup1.

After creating Backup1, you perform the following changes to VM1:

1.

Modify the size of VM1.

2.

Copy a file named Budget.xls to a folder named Data.

3.

Reset the password for the built-in administrator account.

4.

Add a data disk to VM1.

An administrator uses the Replace existing option to restore VM1 from Backup1.

You need to ensure that all the changes to VM1 are restored.

Which change should you perform again?

A. Modify the size of VM1.

B. Reset the password for the built-in administrator account.

C. Add a data disk.

D. Copy Budget.xls to Data.

Correct Answer: D

Reference: https://docs.microsoft.com/en-us/azure/backup/about-azure-vm-restore

QUESTION 3

DRAG DROP

You have an on-premises network that you plan to connect to Azure by using a site-so-site VPN.

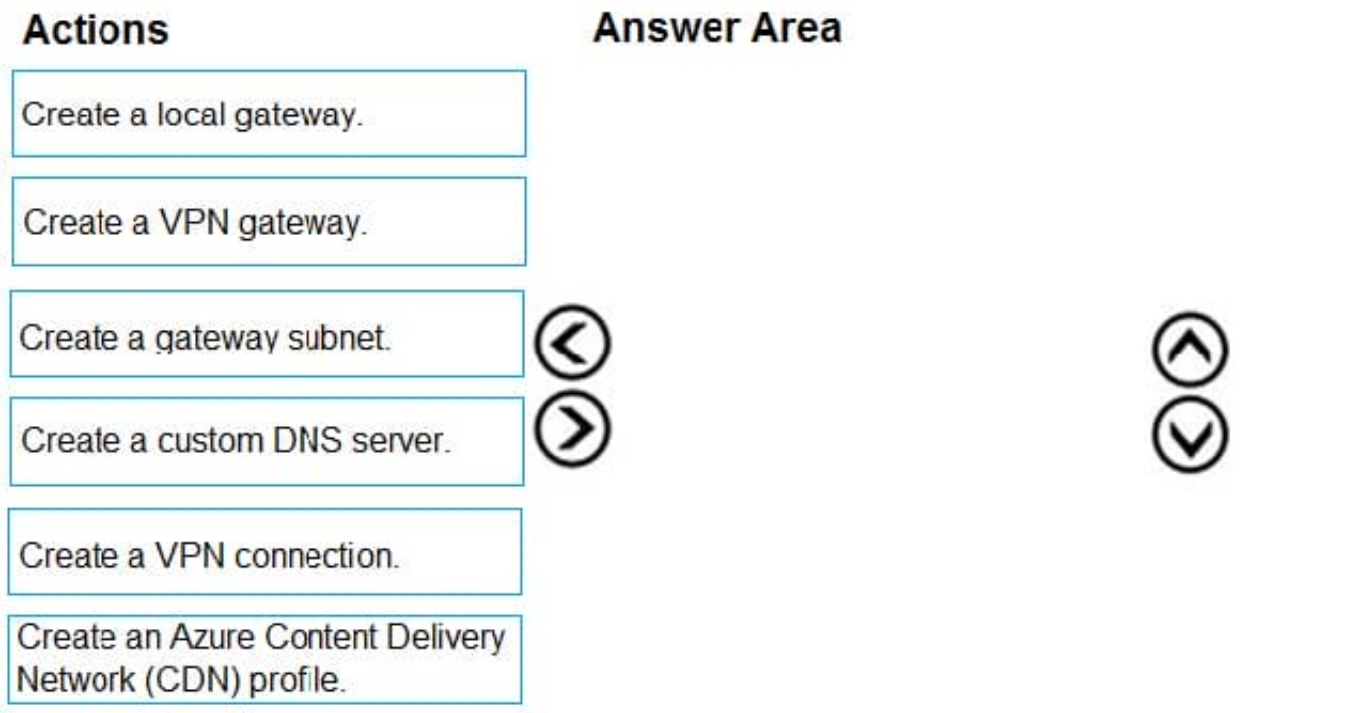
In Azure, you have an Azure virtual network named VNet1 that uses an address space of 10.0.0.0/16 VNet1 contains a subnet named Subnet1 that uses an address space of 10.0.0.0/24.

You need to create a site-to-site VPN to Azure.

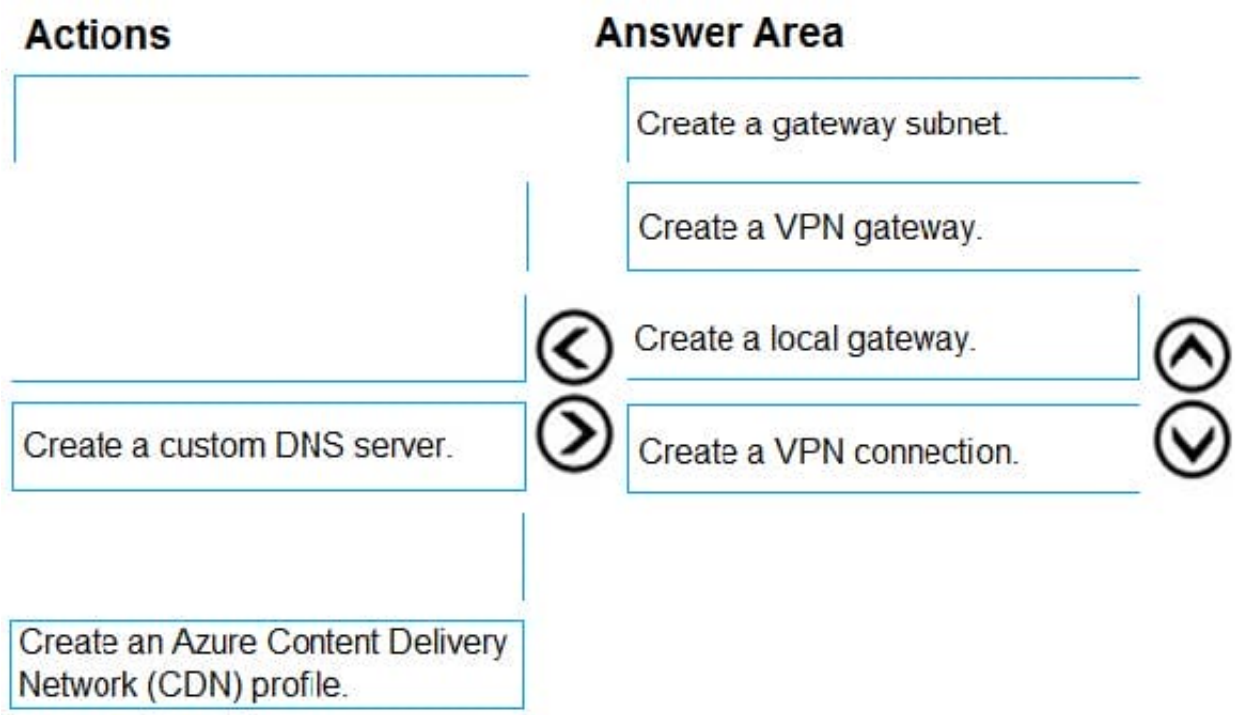
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

NOTE: More than one order of answer choice is correct. You will receive credit for any of the correct orders you select.

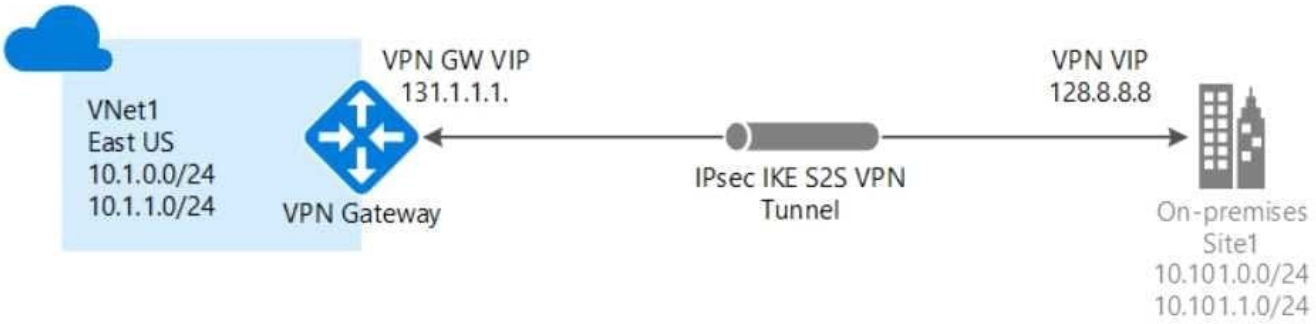
Select and Place:



Correct Answer:



A Site-to-Site VPN gateway connection is used to connect your on-premises network to an Azure virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. This type of connection requires a VPN device located on-premises that has an externally facing public IP address assigned to it. For more information about VPN gateways, see About VPN gateway.



1.

Create a virtual network

You can create a VNet with the Resource Manager deployment model and the Azure portal

2.

Create the gateway subnet :

The virtual network gateway uses specific subnet called the gateway subnet. The gateway subnet is part of the virtual network IP address range that you specify when configuring your virtual network. It contains the IP addresses that the

virtual network gateway resources and services use.

3.

Create the VPN gateway :

You create the virtual network gateway for your VNet. Creating a gateway can often take 45 minutes or more, depending on the selected gateway SKU.

4.

Create the local network gateway:

The local network gateway typically refers to your on-premises location. You give the site a name by which Azure can refer to it, then specify the IP address of the on-premises VPN device to which you will create a connection. You also

specify the IP address prefixes that will be routed through the VPN gateway to the VPN device. The address prefixes you specify are the prefixes located on your on- premises network. If your on-premises network changes or you need to

change the public IP address for the VPN device, you can easily update the values later.

5.

Configure your VPN device:

Site-to-Site connections to an on-premises network require a VPN device. In this step, you configure your VPN device. When configuring your VPN device, you need the following:

A shared key. This is the same shared key that you specify when creating your Site-to-Site VPN connection. In our examples, we use a basic shared key. We recommend that you generate a more complex key to use.

The Public IP address of your virtual network gateway. You can view the public IP address by using the Azure portal, PowerShell, or CLI. To find the Public IP address of your VPN gateway using the Azure portal, navigate to Virtual network

gateways, then click the name of your gateway.

6.

Create the VPN connection:

Create the Site-to-Site VPN connection between your virtual network gateway and your on-premises VPN device.

Reference:

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource- manager-portal

---

QUESTION 4

HOTSPOT

You have an Azure subscription that contains a user named User1 and a storage account named storage1. The storage1 account contains the resources shown in the following table.

Name	Type
container1	Container
folder1	File share
Table1	Table

User1 is assigned the following roles for storage1:

1.

Storage Blob Data Reader

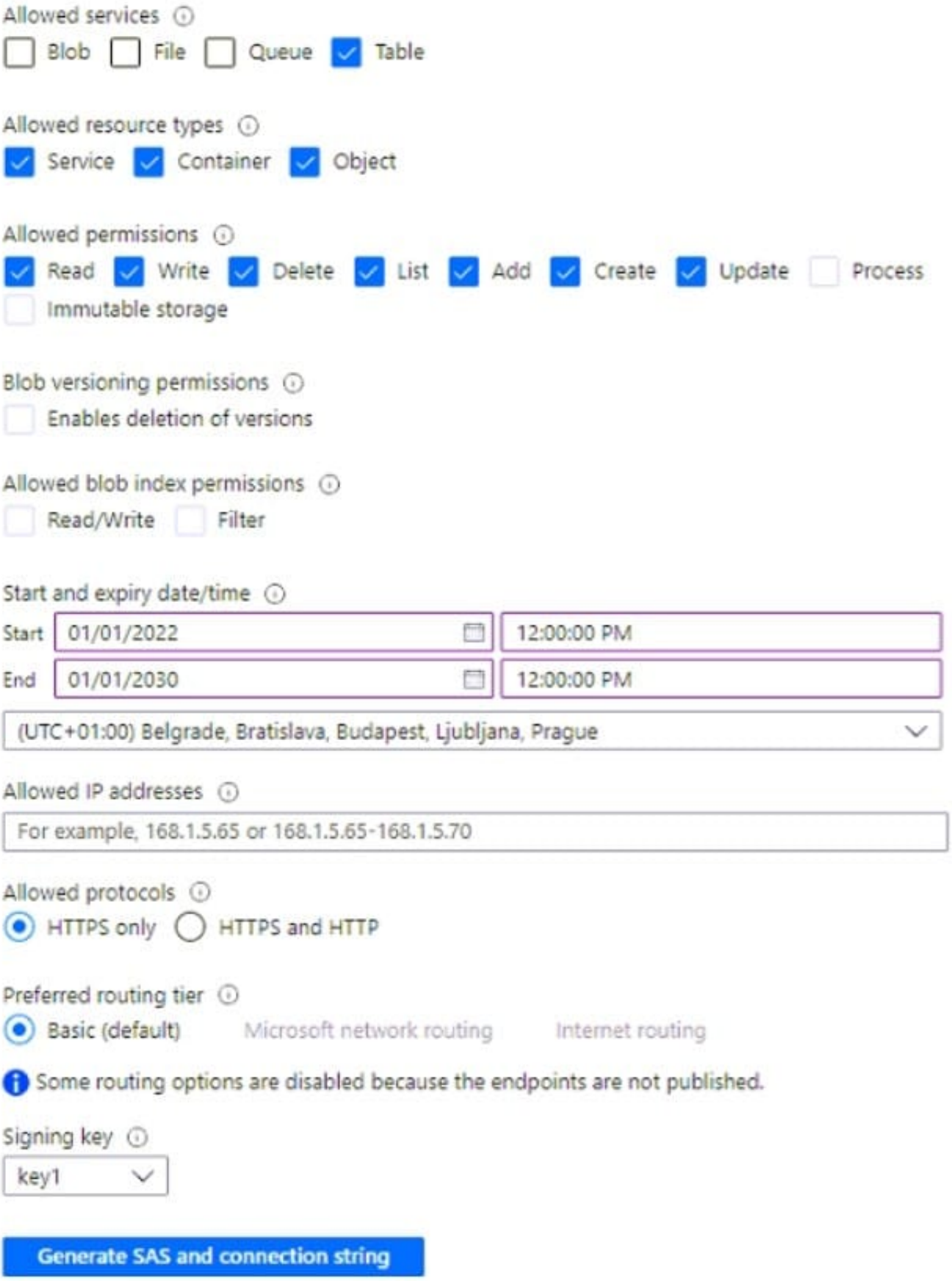
2.

Storage Table Data Contributor

3.

Storage File Data SMB Share Contributor

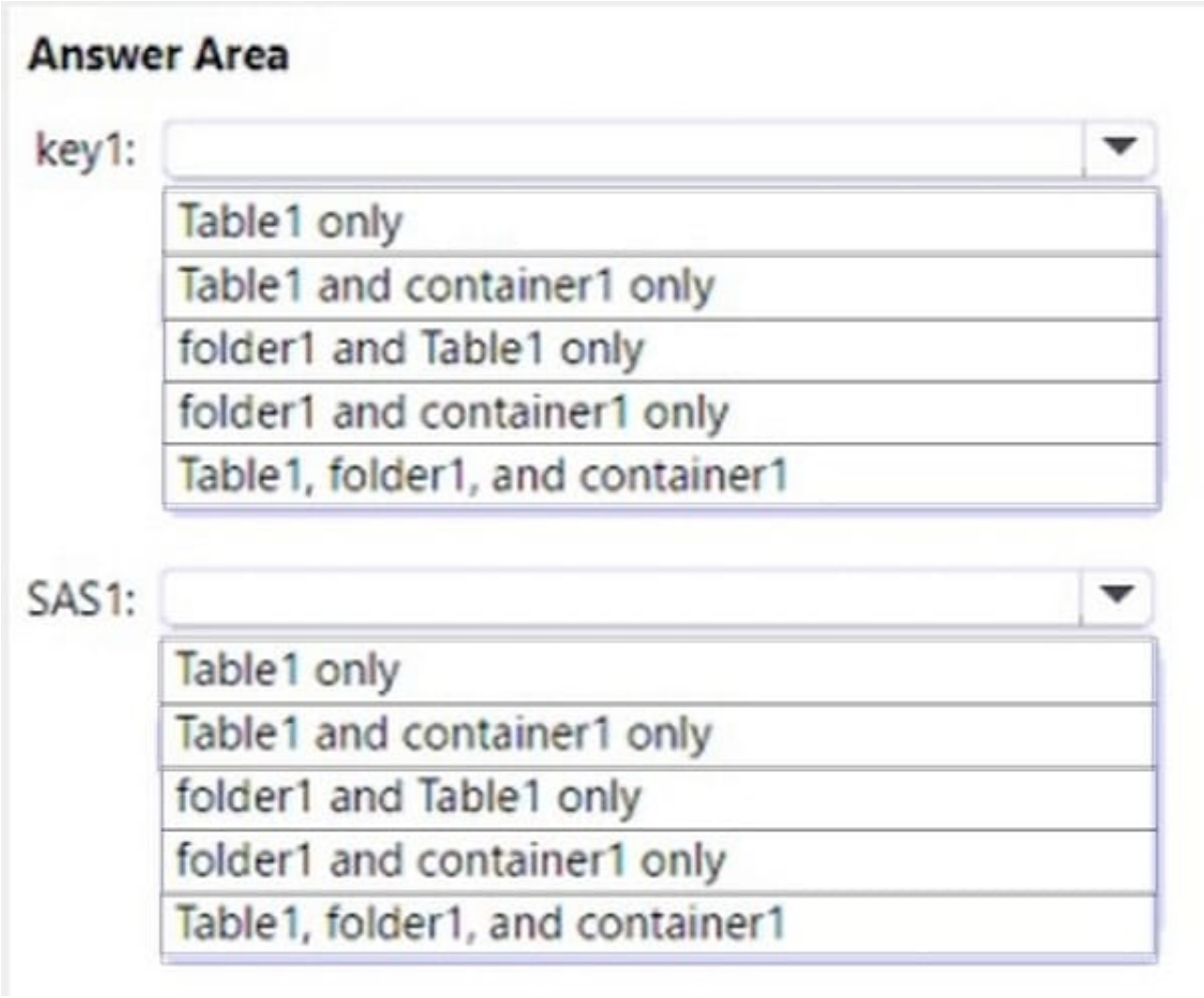
For storage1, you create a shared access signature (SAS) named SAS1 that has the settings shown in the following exhibit. (Click the Exhibit tab.)


Allowed services
Blob
File
Queue
Table
Allowed resource types
Service
Container
Object
Allowed permissions
Read
Write
Delete
List
Add
Create
Update
Process
Immutable storage
Blob versioning permissions
Enables deletion of versions
Allowed blob index permissions
Read/Write
Filter
Start and expiry date/time
Start
01/01/2022
12:00:00 PM
End
01/01/2030
12:00:00 PM
(UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
Allowed IP addresses
For example, 168.1.5.65 or 168.1.5.65-168.1.5.70
Allowed protocols
HTTPS only
HTTPS and HTTP
Preferred routing tier
Basic (default)
Microsoft network routing
Internet routing
Some routing options are disabled because the endpoints are not published.
Signing key
key1
Generate SAS and connection string

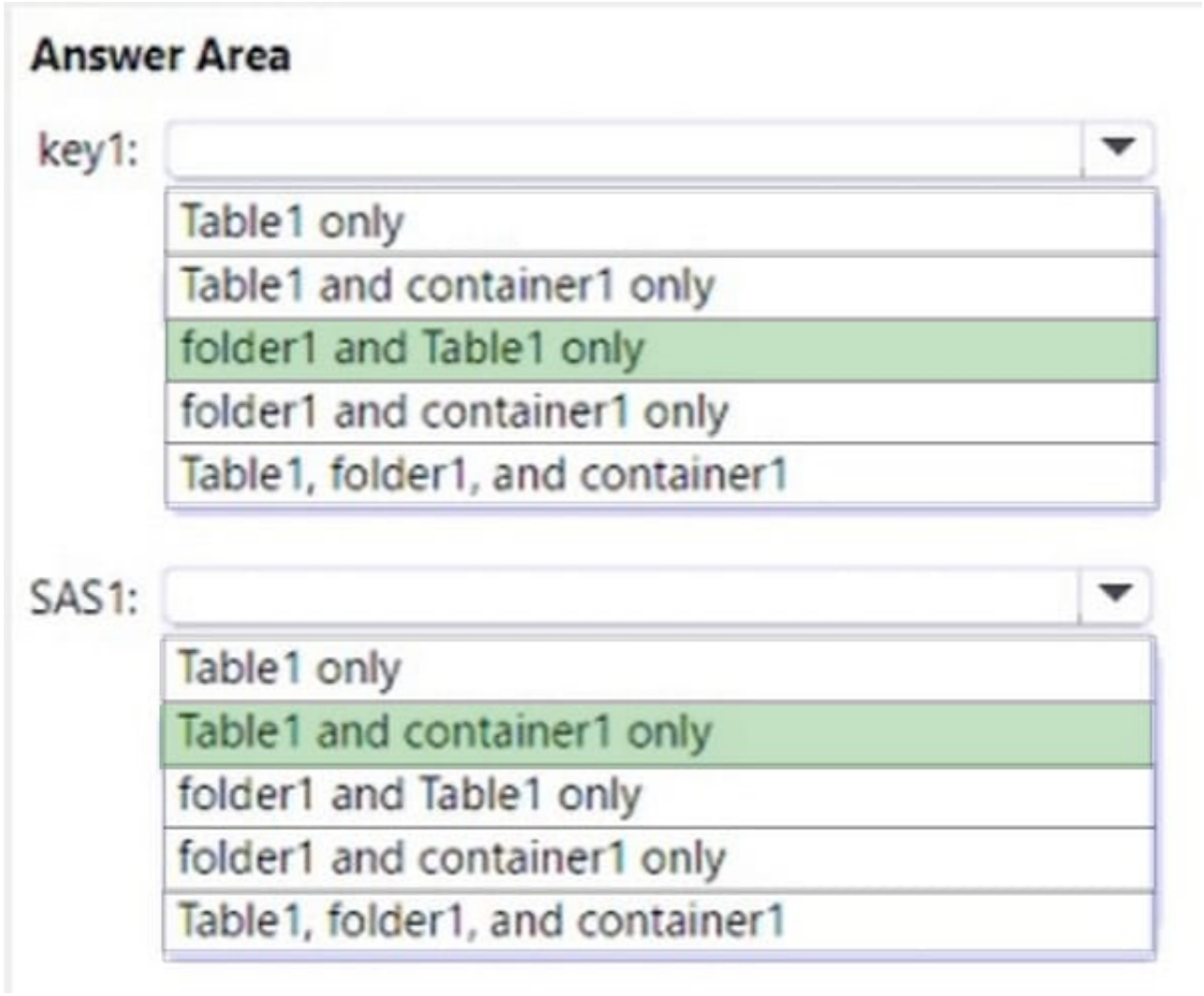
To which resources can User1 write by using SAS1 and key1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: folder1 and Table1 only With key1.

User1 is assigned the following roles for storage1: Storage Blob Data Reader Storage Table Data Contributor Storage File Data SMB Share Contributor

*

Storage Table Data Contributor Allows for read, write and delete access to Azure Storage tables and entities Can write to Table1

*

Storage File Data SMB Share Contributor Allows for read, write, and delete access on files and directories in Azure file shares. Can write to folder1

Box 2: Table1 and container1 only

With SAS1.

For key1 we see:

Allowed services: Table only. Not File, so not folder1.

Allowed resource types: Service, Container, Object.

Allowed permissions: Read, write, etc.

Note: How a shared access signature works

A shared access signature is a signed URI that points to one or more storage resources. The URI includes a token that contains a special set of query parameters. The token indicates how the resources may be accessed by the client. One of

the query parameters, the signature, is constructed from the SAS parameters and signed with the key that was used to create the SAS. This signature is used by Azure Storage to authorize access to the storage resource.

Reference:

https://learn.microsoft.com/en-us/azure/storage/common/storage-sas-overview

https://learn.microsoft.com/en-us/azure/storage/files/storage-files-identity-ad-ds-assign-permissions

QUESTION 5

You have an Azure subscription that contains a storage account named storage1 in the North Europe Azure region.

You need to ensure that when blob data is added to storage1, a secondary copy is created in the East US region. The solution must minimize administrative effort.

What should you configure?

A. operational backup

B. object replication

C. geo-redundant storage (GRS)

D. a lifecycle management rule

Correct Answer: B